DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 31 May 2009

IMSE-KNX-IMA 31 May 2007

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 13-07 – Computer Administrative Rights

1. References.

a. AR 25-2, Information Assurance, 14 November 2003.

b. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

c. Privileged-Level Access Agreement Acceptable Use Policy (AUP), Version 1.0, 06-PR-M-0003, 3 November 2006.

2. Purpose. The Fort Knox automated information systems (i.e., laptops, desktops, and servers) provide the primary automated information infrastructure supporting operational and administrative functions. These systems provide reliable, timely, and direct methods of communicating electronically and storing information essential to daily operations. Technical controls must be adopted to ensure that access to information resources is limited to authorized personnel.

3. Applicability. This policy applies to all Soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to the Fort Knox Campus Area Network.

4. Policy. Administrator privileges are defined as authorized membership in the domain's local administrator or Fort Knox operator group. Administrator privileges authorize access by specific users to processes, computers, computer resources, or protected information.

a. Administrative privileges will **NOT** be granted based on an individual's rank or position.

b. The installation Information Assurance Manager (IAM) is the approval authority for granting administrator privileges.

c. Administrator privileges shall be granted only to individuals who meet **one** of the following criteria:

(1) The individual is appointed as a unit/directorate/organization Information Management Officer or Information Assurance Security Officer; orders must be on file with the installation IAM.

(2) The individual is granted the ability to change system security configurations due to mission requirements (i.e., a functional administrator for a Standard Army Management Information System or a program the user requires for their mission cannot be used without administrator rights).

5. Process.

a. The commander/director must submit a **digitally signed e-mail** to the IAM requesting administrator privileges for an individual. The digitally signed e-mail must include the user's name; workstation name user requires administrative rights to, proof of required training, and a signed FK Form 5077. The user will not receive administrator privileges until the unit commander/director receives approval from the installation IAM.

b. Required Training. All individuals who have administrative privileges must complete the following information assurance courses, which are available at http://ia.gordon.army.mil:

(1) Computer User Security Training (IA Awareness Training).

(2) Information Assurance Security Officer Certification Course, Management Level 1.

c. Privileged-level Access Agreement Acceptable Use Policy (AUP). Each user granted administrator privileges must sign the Privileged-level Access Agreement Acceptable Use Policy (AUP) and a Certificate of Non-disclosure (FK Form 5077).

6. Point of contact is the Installation Information Assurance Manager at 4-5782.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A